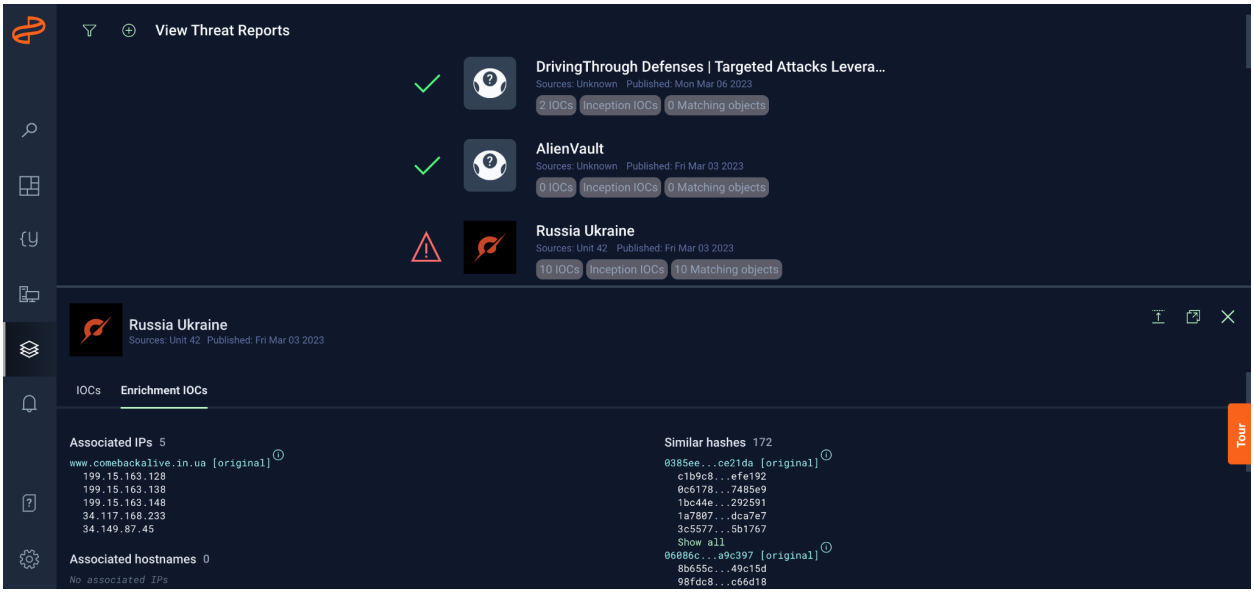
Detect and respond to emerging threats



Stairwell's live threat reports feature allows organizations to upload threat reports and subscribe to threat feeds of interest. The Stairwell platform then extracts indicators of compromise (IOCs), hashes, and YARA rules from the threat reports and scans across a customer's entire file corpus for direct and variant matches. This gives customers confidence in knowing whether their network is affected today and across time. Once a report is in the Stairwell platform, a copy of the report lives forever, making Stairwell an ideal location to act as a repository for all threat intelligence.

Switch to actionable threat intelligence

Customers have an abundance of options for threat intelligence. There are countless paid options and even more open-source feeds available. But the real question is: what does an organization do with this information, and does it deliver value? Stairwell puts threat intelligence to work and allows organizations to autonomously track all relevant malware threats, look across all current files, and continuously scan incoming files to alert on any matches. This allows an organization to understand what threat intel is most relevant and how it can be used elsewhere in the security stack.

Clean bill of health

Stairwell's live threat reports answers the question, "is my organization affected by [name your threat]?" in near real-time. Additionally, organizations will know if they ever become susceptible to the threat of interest through automated retroactive scanning.

Detect known and unknown threats

Most novel malware is a variant of an existing malware family. Stairwell allows you to discover variants before they are part of a threat report. Analysts will have a real-time view if these variants are present today or at any time in the future. This drastically reduces the time threat researchers have to spend on identifying and searching for variant IOCs.

Live threat reports data sheet

How does this work?

Stairwell ingests threat reports and stores them across time. IOCs get extracted and scans are performed across every file an organization has uploaded, giving security practitioners near real-time results. Additionally, Stairwell identifies and scans for variant hashes, IPs, and hostnames, which gives even greater visibility into known and novel malware threats. Any time a new file is uploaded, it's scanned against the repository of threat intelligence which gives an analyst the power to always understand susceptibility to malware threats.

Live threat reports use cases

Organizational susceptibility	Unfortunately, the next big attack is a matter of when, not if. Threat reports gives you confidence in always knowing if you're at risk.
Software supply chain attacks	Monitor vendor-supplied executables for threats and vulnerabilities, giving unique visibility into your supply chain.

Live threat reports key features and benefits

Feature	**Benefit**
Report repository	Always have a copy of your threat reports and build out your organization's threat intelligence.
Triggers and notifications	Get notified directly into your SIEM/SOAR/SOC dashboard if files or variants ever match your threat intelligence.
Discover variant intelligence	Most "new" malware is a variant of a past version. Stay ahead of attackers by looking for variants before they are known threats.
Continuous scanning	Upload reports once to get historical and future alerts.
IOC tuning	Customize IOC and alert behavior to focus on what's most important to your organization.

Learn more about the Stairwell platform

To learn more about how the Stairwell platform helps you detect and defend against supply-chain attacks beyond what traditional security tools offer, contact us.